le: 4410-NW

DEPARTMENT OF JUSTICE

[CPCLO Order No. 007-2021]

Privacy Act of 1974; Systems of Records

AGENCY: Justice Management Division, United States Department of Justice.

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Justice Management Division (JMD), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled Security Monitoring and Analytics Service Records, JUSTICE/JMD-026. JMD proposes to establish this system of records to provide external federal agency subscribers with the technical capability to protect their data from malicious or accidental threats using DOJ-managed systems.

DATES: In accordance with 5 U.S.C. 552a (e) (4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments: by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, 145 N St. NE, Suite 8W.300, Washington, DC 20530; by facsimile at 202-307-0693; or by email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION:

In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, agencies are responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017), directs agency heads to show preference in their procurement for shared information technology (IT) services, to the extent permitted by law, including email, cloud, and cybersecurity services. Office of Management and Budget (OMB) Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government (April 26, 2019), establishes the framework for implementing "Sharing Quality Services" across agencies. The Economy Act of 1932; 31 U.S.C. 1535, authorizes agencies to enter into agreements to obtain supplies or services from another agency.

Consistent with these authorities, the JMD, Office of the Chief Information Officer (OCIO), Cybersecurity Services Staff (CSS), developed the Security Monitoring and Analytics Service (SMAS) system to provide DOJ-managed IT service offerings to other federal agencies wishing to leverage DOJ's cybersecurity services, referred to as "external federal agency subscribers." SMAS has a suite of technology products, which consists of a range of commercial off-the-shelf (COTS) software that provide insight into the subscribers' operating environment. SMAS capabilities include, but are not limited to, asset discovery, vulnerability assessment, Network Intrusion Detection System (NIDS), Endpoint Detection and Response (EDR), and Security Information and Event Management (SIEM) event correlation and log management. SMAS also offers User Behavior Analytics (UBA) and User Activity Monitoring (UAM) tools to correlate security events, as part of the service offering. SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity that may indicate malicious behavior and activity. DOJ provides this information directly to external federal agency subscribers for review

and further evaluation. JMD monitors user activities and captures and stores files that might be related to suspicious, unauthorized, or anomalous activities. JMD ensures that possible security events or incidents are accurately identified, analyzed, guarded against, investigated, and shared with the external federal agency subscriber via secure means of communication (e.g., encrypted email).

JMD established the system of records, Security Monitoring and Analytics Service Records, JUSTICE/JMD-026, to cover records maintained by JMD while utilizing SMAS for its external federal agency subscribers. Specifically, JMD tracks external federal agency subscriber's IT, information system, and/or network activity, including any access by users to any IT, information systems, and/or networks, whether authorized or unauthorized. Consistent with these requirements, JMD must ensure that it maintains accurate audit and activity records of the observable occurrences on external federal agency subscriber information systems and networks (also referred to as "events") that are significant and relevant to the security of the external federal agency subscriber's information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. These records assist DOJ and external federal agency subscribers with protecting subscribers' data and ensuring the secure operation of IT, information systems, and networks.

Additionally, monitored events—whether detected utilizing information systems maintaining audit and activity records, reported to the Department or external federal agency subscriber by information system users, or reported to the Department or the external federal agency subscriber by the cybersecurity research community or members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent

threat of violation of law, security policies, security procedures, or acceptable use policies. These records assist DOJ and external federal agency subscribers with tracking and documenting actual or suspected incidents, which may, in limited circumstances, include records of individuals reporting, or otherwise associated with, an actual or suspected incident.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: July 20, 2021

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice

JUSTICE/JMD-026

SYSTEM NAME AND NUMBER:

Security Monitoring and Analytics Service Records, JUSTICE/JMD-026

SECURITY CLASSIFICATION:

Controlled Unclassified Information

SYSTEM LOCATION:

Records will be maintained electronically at Department of Justice offices, other sites utilized by the Department of Justice, and in information technology, information systems, or networks owned, operated by, or operated on behalf of the Department of Justice. Most records will be maintained electronically at one or more of the Department's Core Enterprise Facilities (CEF), including, but not limited to: CEF East, Clarksburg, WV 26306; CEF West, Pocatello, ID 83201; or CEF-DC, Sterling, VA 20164. In the future, records may also be maintained by a Department-authorized cloud service provider if the Department decides that so doing will provide increased security and accessibility. In that event, any servers would be maintained within the Continental United States and the name and address of the Department-authorized cloud service provider will be made public, and for purposes of individual access and amendment, the location of the records will continue to be at the address listed above.

Some or all system information may also be duplicated at other locations where the Department has granted direct access to support DOJ System Manager operations, system backup, emergency preparedness, and/or continuity of operations. For more specific information about the location of records maintained in this system of records, contact the system manager using the contact information listed in the "SYSTEM MANAGER(S)" paragraph, below.

SYSTEM MANAGER(S):

DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq*.; The Economy Act of 1932, as amended, 31 U.S.C.1535; Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017).

PURPOSE(S) OF THE SYSTEM:

The Department of Justice (DOJ) Security Monitoring and Analytics Service (SMAS) provides DOJ-managed cybersecurity services to external federal agency subscribers, giving subscribers the technical capability to protect their information, information technologies, information systems, and networks from malicious or accidental threats. SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity and/or vulnerabilities. Records in this system of records are used by system administrators and security personnel, or persons authorized to assist these personnel, for the purpose of: reviewing and analyzing subscriber information and subscriber information system activity and access events for indications of inappropriate, unusual, or abnormal activity; tracking, documenting, and handling actual or suspected cybersecurity events and incidents; identifying and managing vulnerabilities; supporting audit reviews, analyses, reporting requirements, and after-the-fact investigations of cybersecurity events and incidents; planning and managing system services; and otherwise performing their official duties. Authorized personnel may use the records in this system for the purpose of investigating improper access or other improper activity related to information system access; and referring such record(s) to external federal agency subscribers.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. SMAS authorized users, including DOJ employees, DOJ contractors, and employees and contractors of external federal agency subscribers with authorized access to SMAS to perform analysis on collected information; and

B. The categories of individuals covered by this system encompass all individuals who are provided external federal agency subscriber information technology monitored by SMAS, who access external federal agency subscriber information systems monitored by SMAS, or who

transmit information across external federal agency subscriber networks monitored by SMAS. Such individuals may include: 1) individuals who use external federal agency subscriber information technology, information systems, and/or networks to send or receive information or related communications, access Internet sites, or access any external federal agency subscriber information technologies, information systems, or information; 2) individuals from outside the external federal agency subscriber who communicate electronically with subscriber users, information technologies, information systems, and/or networks; 3) individuals reporting, tracking, documenting and/or otherwise associated with actual or suspected cybersecurity incident and/or event activities; and 4) any individuals who attempt to access external federal agency subscriber information technologies, information systems, and/or networks, with or without authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records may include:

A. Access and activity logs that establish what type of event occurred, when an event occurred, where an event occurred, the source of an event, the outcome of an event, and the identity of any individuals or subjects associated with an event. Such information includes, but is not limited to: time stamps recording the data and time of access or activity; source and destination addresses; user, device, and process identifiers, including Internet Protocol (IP) address, Media Access Control (MAC) address, and event descriptions; success/fail indications; filenames involved; full text recording of privileged commands; and/or access control or flow control rules invoked. Such information may be collected and aggregated by the operating system or application software locally within an information technology, information system, or network.

B. Information relating to any individuals accessing an external federal agency subscriber's information, information technologies, information systems, or networks monitored by SMAS. This includes: user names; persistent identifiers (such as a User ID); contact

information, such as title, office, component, and agency; and the authorization of an individual's access to systems, files, or applications, such as signed consent forms or Rules of Behavior forms, or access authentication information (including but not limited to passwords, challenge questions/answers used to confirm/validate a user's identity, and other authentication factors).

C. Records on the use of electronic mail, instant messaging, other chat services, electronic call detail information (including name, originating/receiving numbers, duration, and date/time of call), and electronic voicemail on an external federal agency subscriber's information technologies, information systems, or networks monitored by SMAS.

D. Records of Internet access from any information technology connected to an external federal agency subscriber's information system or network monitored by SMAS, or through authorized connections to external federal agency subscriber's networks and information systems monitored by SMAS, including the IP address of the information technology being used to initiate the Internet connection and the information accessed.

E. Audit reviews, analyses, and reporting, including but not limited to, audits that result from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, physical access, and communications at the boundaries of information systems monitored by SMAS.

F. Actual or suspected incident or event report information, including but not limited to: information related to individuals reporting, tracking, documenting, and/or otherwise associated with a cybersecurity incident and/or event; information related to reporting, tracking, investigating, and/or addressing an incident or event (e.g., data/time of the incident or event; location of incident or event; type of incident or event; storage medium information; safeguard information; external/internal entity report tracking; data elements associated with the incident or event; information on individuals impacted; information on information system(s) impacted; remediation, response, or notification actions; lessons learned; risk of harm and compliance

assessments); and information related to discovering, testing, reporting, tracking, investigating, and/or addressing a security vulnerability or indicator of a security vulnerability.

RECORD SOURCE CATEGORIES:

Records covered by this system of records are generated internally (i.e., information technology, information system, and/or network activity logs), manually sourced from agency personnel, or sourced directly from the individual to whom the record pertains.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. To an organization or individual in both the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy or other threat, to the extent the information is relevant to the protection of life, health, or property. Information may be similarly disclosed to other recipients who share the same interests as the target or who may be able to assist in protecting against or responding to the activity or conspiracy.

B. To appropriate officials and employees of a federal agency for which the Department is authorized to provide a service, when disclosed in accordance with an interagency agreement and when necessary to accomplish an agency function articulated in the interagency agreement.

C. To any person(s) or appropriate Federal, state, local, territorial, tribal, or foreign law enforcement authority authorized to assist in an approved investigation of or relating to the improper usage of DOJ information technologies, information systems, and/or networks.

D. To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

E. To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

F. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

G. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

H. To any person or entity that the Department has reason to believe possesses information regarding a matter within the jurisdiction of the Department, to the extent deemed to be necessary by the Department in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

I. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

J. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

K. To the news media and the public, including disclosures pursuant to 28 CFR § 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

L. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, interagency agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

M. To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

N. To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

O. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

P. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

Q. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

R. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

S. To another federal agency or entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

T. To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of DOJ, and meeting related reporting requirements.

U. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic storage media, in accordance with the safeguards mentioned below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Data shared with the external agency subscriber consists of report(s) on the automated alerts generated by the tools or manually collected through the hotline. At the request of the external agency subscriber, DOJ can provide custom reports, which may be grouped by username, host name, IP address or another key indicator. Records may be retrieved by identifying characteristics as part of information system security monitoring, cybersecurity incident response, user activity monitoring, or in support of other security activity.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 3.2: Information Systems Security Records, Transmittal No. 26 September 2016, item 010–062 and General Records Schedule 5.6: Security Records, Transmittal No. 31 April 2020, item 210–240, for records created and maintained by federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. Log data is maintained in Logging as a Service as the DOJ's repository for 365 days.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in this system is safeguarded in accordance with appropriate laws, rules, and policies, including the Department's automated systems security and access policies and Interconnection Security Agreements (ISAs) with the federal agency subscribers. Access to such information is limited to Department personnel, contractors, and other personnel who have an official need for access in order to perform their duties. Records are maintained in an access-controlled area, with direct access permitted to only authorized personnel. Electronic records are accessed only by authorized personnel with accounts on the Department's network. Additionally, direct access to certain information may be restricted depending on a user's role and responsibility within the organization and system. Any electronic data that contains personally identifiable information will be encrypted in accordance with applicable National Institute of Standards and Technology standards when transferred between DOJ and the subscriber agency.

RECORD ACCESS PROCEDURES:

A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR Part 16, and should be sent by mail to the Justice Management Division, ATTN: FOIA Contact, Room 1111, Robert F. Kennedy Department of Justice Building, 950 Pennsylvania Avenue, N.W., Washington, DC 20530-0001, or by email at *JMDFOIA@usdoj.gov*. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity from the FOIA/Privacy Act Mail Referral Unit, Justice Management Division, United States Department of Justice, 950 Pennsylvania Avenue N.W., Washington, DC 20530–0001, or from the Department's Web site at *http://www.justice.gov/oip/forms/cert_ind.pdf*. Some information may be exempt from the access provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system may access any stored records that are not exempt from the access provisions. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend information maintained in the system should direct their requests to the address indicated in the "RECORD ACCESS PROCEDURES" section, above. The envelope and letter should be clearly marked "Privacy Act Amendment Request." The request must comply with 28 CFR § 16.46, and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below.

An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General will promulgate regulations exempting this system of records from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that information in the system of records is subject to exemption, pursuant to 5 U.S.C. 552a(k)(2). The Department is in the process of promulgating regulations in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), that will be published in the Federal Register.

HISTORY:

None.

[FR Doc. 2021-15883 Filed: 7/29/2021 8:45 am; Publication Date: 7/30/2021]